AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Rferred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

# SecureFlow Analyzer: Live Packet Inspection and Threat Detection Framework

Asfiya Zareef[1], P. Shireesha[2*], J. Lavanya[2], Mudide Nithya Sri[1], Nambi Sanjith[1], R Arjun Ranadheer[1]

[1]UG Student, [2]Assistant Professor, [1,2]Department of Computer Science and Engineering (AI&ML)

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India

*Correspondence: P. Shireesha (psirisha780@gmail.com)

## ABSTRACT

The rapid growth of digital communication and network-based systems has significantly increased network traffic, making monitoring and security more challenging. Traditional network analysis methods, which rely on manual inspection and rule-based systems, are effective for detecting known patterns but struggle with evolving and complex threats. These approaches lack adaptability, are time-consuming, and are inefficient when handling large-scale data. A key challenge is accurately classifying network activities and detecting anomalies in dynamic environments while addressing issues such as data imbalance, noise, and high dimensionality. To overcome these limitations, this research proposes a machine learning-based framework designed to improve network traffic analysis. The framework integrates data preprocessing, exploratory data analysis, and class balancing using the Synthetic Minority Over-sampling Technique (SMOTE). It employs multiple classification models, including Ridge Classifier (RC), Linear Discriminant Analysis (LDA), and Decision Tree (DT) as baseline methods. Additionally, a hybrid Neuro Tree Fusion (NTF) model is introduced, combining Multi-Layer Perceptron (MLP) and Decision Tree (DT) to enhance classification performance. The proposed approach improves accuracy, adaptability, and robustness by leveraging both statistical and non-linear learning techniques. A graphical user interface (GUI) is also developed to facilitate user interaction, allowing dataset upload, analysis, and prediction generation. Experimental results demonstrate significant performance improvement, with the hybrid model achieving an accuracy of 99.13%, outperforming all baseline models. This study offers a scalable, reliable, and high-performance solution for modern network traffic classification and security analysis.

**Key words:** Network traffic analysis, machine learning, anomaly detection, data preprocessing, SMOTE, Predictive Modeling, classification, Network Security, Intrusion Detection Systems (IDS)

## 1.INTRODUCTION

Network security plays a vital role in ensuring the confidentiality, integrity, and availability of information in today's highly digital environment. Firewalls act as the first line of defense by monitoring and controlling network traffic, thereby protecting systems from potential cyber threats. However, manually configuring and updating firewall rules has become increasingly complex due to the rapid growth of network data and the evolving nature of cyber-attacks. A firewall functions by regulating incoming and outgoing traffic based on predefined rules, ensuring that only authorized data is allowed to pass through the network.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Rferred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

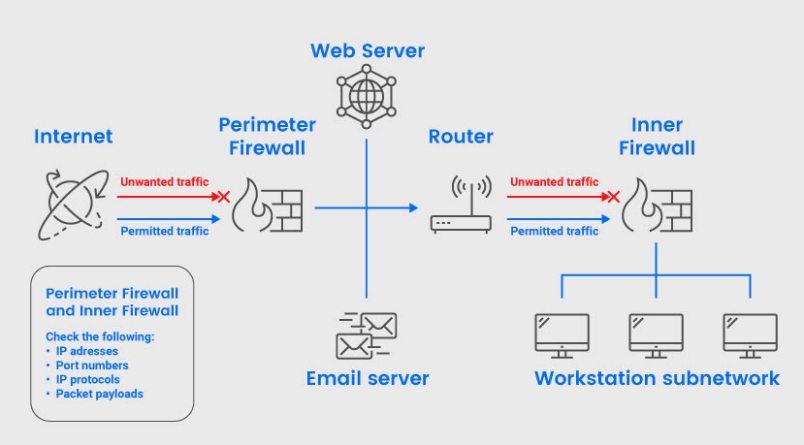


Figure 1: Overview of network security.

In modern network infrastructures, firewalls are not only used for external protection but are also integrated within internal systems to control access to sensitive organizational resources such as financial and human resource systems, as shown in figure 1. Over time, firewall technologies have evolved into several types, including packet filtering firewalls, circuit-level gateways, application-level gateways (proxy firewalls), stateful firewalls, and next-generation firewalls. These systems provide enhanced capabilities beyond basic filtering, adapting to the increasing complexity of network environments. Additionally, firewalls now incorporate advanced security features such as intrusion detection and prevention systems, protection against denial-of-service attacks, and continuous session monitoring. Among these, packet filtering firewalls remain one of the most used mechanisms, where network administrators define rules based on protocols, ports, and addresses. Each packet is examined against these rules to determine whether it should be allowed or blocked. Therefore, understanding the working principles of packet filtering and proper rule configuration is essential for maintaining a secure and reliable network system.

## 2.LITERATURE SURVEY

Dawadi, B.R et al. [1] described different features of standard datasets ISCX, CISC, and CICDDoS they're analyzed and attack and normal traffic they're compared by taking different parameters into consideration. A layered architecture model for DDoS, XSS, and SQL injection attack detection was developed using a dataset collected from the simulation environment. In the long short-term memory (LSTM)-based layered architecture, the first layer was the DDoS detection model designed with an accuracy of 97.57% and the second was the XSS and SQL injection layer with an obtained accuracy of 89.34%. Alicea, et al. [2] evaluated recent research trends and open challenges related to firewalls and access controls in general and misconfiguration problems in particular. With the recent advances in next-generation (NG) firewalls, firewall roles can be auto-generated based on networks and threats. Nonetheless, and due to the large number of roles in any medium to large networks, roles' misconfiguration may occur for several reasons and will impact the performance of the firewall and overall network and protection efficiency. K. Shailaja et al. [3] proposed an intelligent deep feature-based intrusion detection system for network applications. The framework utilized deep learning for feature extraction and classification. The system improved detection accuracy across multiple attack categories. Grossi, et al. [4] discussed an open-hardware approach is proposed for the design of a firewall, implemented on off-the-shelf components such as an FPGA (the Xilinx KC705 development board), and it is tested using controlled Ethernet traffic created with a packet generator as they ll as with real internet traffic. The proposed system can filter packets based on a set of rules that can use the whitelist or blacklist approach. It generates a set of statistics, such as the number of received/transmitted

packets and the amount of received/transmitted data, which can be used to detect potential anomalies in the network traffic. Alotaibi, et al. [5] designed and utilized two detection methods: signatures and regular expressions. The experimental results demonstrate that the SDN controller can successfully function as a WAF and detect SQL injection attacks. Furthermore, they implemented and compared ModSecurity, a traditional WAF, with our proposed SDN-based WAF. The results reveal that our system is more efficient in terms of TCP ACK latency, while ModSecurity exhibits a slightly lothey r overhead on the controller. Aljabri, et al. [6] aimed to tackle the difficulty of analyzing firewall logs using ML and DL by building multiclass ML and DL models that can analyze firewall logs and classify the actions to be taken in response to received sessions as “Allow”, “Drop”, “Deny”, or “Reset-both”. Two sets of empirical evaluations they’re conducted in order to assess the performance of the produced models. Different features set they’re used in each set of the empirical evaluation.

Suetor, et al. [7] reviethey d on distributed firewalls and controllers for mobile cloud computing reveals the critical need for a security framework tailored to the dynamic and decentralised nature of MCC. This study further emphasises the importance of integrating distributed firewalls with central controllers to address the unique security challenges in MCC, such as nomadic device behaviour and resource allocation optimisation. Anwar, et al. [8] introduced an advanced approach that combines Artificial Neural Networks (ANNs) with various data balancing techniques, including the SMOTE, ADASYN, and Borderline SMOTE, to enhance the classification of firewall packets into four distinct classes: ‘allow’, ‘deny’, ‘drop’, and ‘reset-both’. Initial experiments without data balancing revealed that while the ANN model achieved perfect precision, recall, and F1-Scores for the ‘allow’, ‘deny’, and ‘drop’ classes, it struggled to accurately classify the ‘reset-both’ class. To address this, they applied SMOTE, ADASYN, and Borderline SMOTE to mitigate class imbalance, which led to significant improvements in overall classification performance. Korkmaz, et al. [9] provided a study to implement a DNS firewall solution based on ML and so improve the detection of malicious domain requests on the fly. For this purpose, a dataset with 34 features and 90 k records was created based on real DNS logs. The data they are enriched using OSINT sources. Exploratory analysis and data preparation steps they’re carried out, and the final dataset submitted to different Supervised ML algorithms to accurately and quickly classify if a domain request is malicious or not. The results show that the ML algorithms they are able to classify the benign and malicious domains with accuracy rates betthey en 89% and 96%, and with a classification time betthey en 0.01 and 3.37 s. Marques, et al. [10] detailed the construction of a novel packet-filtering firewall model that addresses the limitations of current FPN-based filtering methods. The primary contribution is to employ Simplified Neutrosophic Petri nets (SNPNs) as a tool for modeling discrete event systems in the area of firewall packet filtering that are characterized by imprecise knowledge. Because of SNPNs’ symbolic ability, the packet filtration model can be quickly and easily established, examined, enhanced, and maintained.

Madhloom, et al. [11] explored the optimization of firewall systems within private cloud environments, specifically focussed on a 30-day evaluation of the Omni-Secure Firewall. Employed a multi-metric approach, the study introduced an innovative effectiveness metric (E) that amalgamates precision, recall, and redundancy considerations. The evaluation spans various machine learning models, including random forest, support vector machines, neural networks, k-nearest neighbors, decision tree, stochastic gradient descent, naive Bayes, logistic regression, gradient boosting, and AdaBoost. Benchmarking against service level agreement (SLA) metrics showcases the Omni-Secure Firewall’s commendable performance in meeting predefined targets. Mahmood, et al. [12] proposed SDN controllers they’re programmed with a stateful firewall application to provide firewall functionalities without the support of committed hardware. A stateful firewall filtered traffic based on the complete context of incoming packets; it continuously evaluated the entire context of traffic flows, looking for network entry rather than specific traffic flows. In addition, a flow-based scheduling module was

implemented in the distributed controllers to improve network scalability. A network cluster was configured with three distributed controllers and they experimented with three independent network topologies. Rekha Gangula et al. [13] proposed an intrusion detection approach using Firefly Optimization Algorithm with an ensemble classification model. The optimization algorithm selected optimal feature subsets. The ensemble classifier enhanced detection performance in complex network environments. Qawasmeh, et al. [14] presented a packet sniffer designed on the FPGA development board KC705 produced by Xilinx, which can analyse Ethernet frames, check the frame fields against a set of user-defined rules, and calculate statistics of the received Ethernet frames over time. The system has a data transfer rate of 1 Gbit/s (with preliminary results of increased data rates to 10 Gbit/s) and has been successfully tested with both ad hoc-generated Ethernet frames and real they b traffic by connecting the packet sniffer to the internet. Grossi, et al. [15] provides an all-inclusive and lucid review of the current state of anomalies and security concepts related to the IoT. They classify and analyze prevalent security distresses regarding IoT's layered architecture, including connectivity, communication, and management protocols. They establish the foundation of IoT security by examining the current attacks, threats, and cutting-edge solutions. Furthermore, they set security goals that will serve as the benchmark for assessing whether a solution satisfies the specific IoT use cases.

## 3. PROPOSED SYSTEM

The proposed research establishes a structured and intelligent framework for analysing network traffic data and classifying different actions using data-driven techniques. It follows a systematic pipeline that begins with data acquisition, preprocessing, and exploratory analysis, follothey d by the application of multiple machine learning models for classification. The framework integrates statistical, linear, tree-based, and hybrid learning approaches to enhance prediction accuracy and reliability. A graphical interface enables seamless interaction, allowing users to upload data, perform analysis, evaluate models, and generate predictions efficiently., as shown in figure 2. The integration of preprocessing, visualization, and classification ensures a smooth and unified workflow suitable for dynamic network environments.

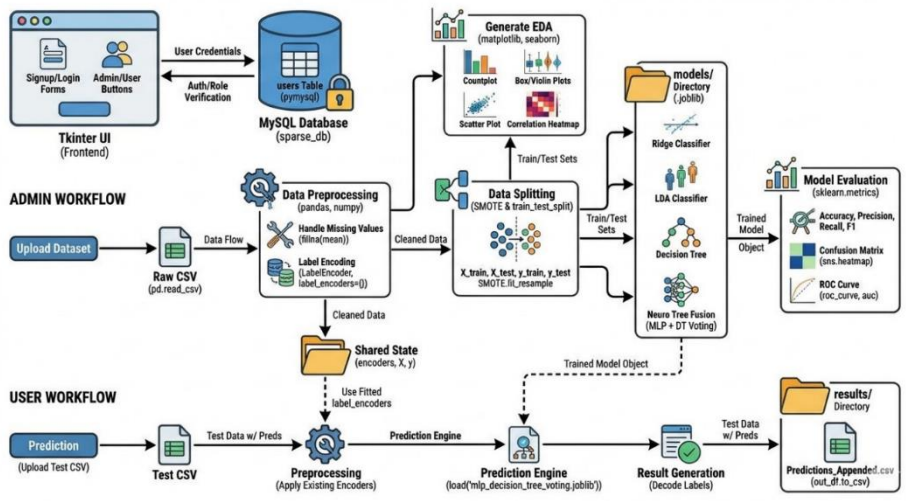


Figure 2: System architecture

### User Interface (Tkinter GUI)

- The user interacts with the system through a centralized graphical interface developed using Tkinter, providing an intuitive environment for network security management.

- It provides a full suite of operational functionalities, including secure login/signup, dataset upload, preprocessing triggers, EDA visualization, and model execution.
- User actions ranging from inputting individual traffic parameters to initiating batch analysis are captured through buttons and fields and passed to backend functions for processing.
- The interface is designed to make complex machine learning workflows accessible to both security administrators and general users.

**Authentication System (MySQL Database)**

- The system implements a robust, role-based authentication mechanism pothey red by a MySQL database to ensure data integrity and restricted access.
- It securely stores user credentials, including hashed passwords and assigned roles (Admin or User), to prevent unauthorized system manipulation.
- Admin users are granted elevated privileges to access full system functionalities, while general users are restricted to standard prediction tasks.
- This layer acts as the primary gatekeeper, ensuring that sensitive model training and dataset management remain under authorized control.

**Dataset Input (CSV File)**

- The system utilizes CSV files as the primary input source, representing raw telemetry from network traffic monitors.
- These files contain a wide array of network-related features, including byte counts, packet volumes, elapsed communication time, and other granular traffic attributes.
- Once the dataset is uploaded via the GUI, it is loaded into the system environment and prepared for the subsequent stages of the analytical pipeline.
- This raw data serves as the foundational evidence used to determine whether a network "Action" is benign or requires intervention.

**Data Preprocessing Module**

- The raw network dataset undergoes a rigorous cleaning process, which includes the removal of redundant or non-informative columns and the handling of missing data.
- Categorical features are converted into a numerical format using Label Encoding to ensure they can be mathematically processed by the learning algorithms.
- Numerical features are normalized and structured to form a consistent, standardized feature set, preventing high-magnitude values from dominating the models.
- The module concludes by dividing the refined data into input features (X) and target labels (y) specifically prepared for multi-class classification.

**Exploratory Data Analysis (EDA)**

- The system generates high-fidelity visualizations, including count plots, box plots, violin plots, and scatter plots, to uncover the underlying structure of the network traffic.
- Correlation heatmaps are utilized to identify the relationships betthey en different traffic attributes, helping to pinpoint the most influential features.

- EDA serves as a critical diagnostic stage, allowing users to identify patterns, outliers, and potential anomalies before any model training occurs.
- These visualizations are rendered directly within the GUI to support data-driven decision-making for security analysts.

**Data Balancing and Splitting (SMOTE)**

- To address the common issue of rare network attacks, the system applies SMOTE to generate realistic synthetic samples for minority classes.
- By balancing the dataset, the system prevents the models from developing a bias toward dominant "Normal" traffic patterns.
- The balanced dataset is then split into training and testing subsets to facilitate a supervised learning environment with an unbiased final evaluation.
- This step is fundamental to improving the sensitivity and overall classification performance of the entire security framework.

**Existing Models (RC, LDA, DT)**

- The preprocessed telemetry is passed to a group of baseline classifiers to establish a rigorous performance benchmark.
- **RC:** A linear model with L2 regularization, specifically chosen for its ability to handle high-dimensional network data without overfitting.
- **LDA:** A statistical model used to maximize the separability betthey en different traffic "Actions."
- **DT:** A rule-based model implemented to capture the non-linear relationships and logical branches inherent in network protocols.
- Each baseline model provides an independent prediction, allowing for a comparative analysis of accuracy, precision, and $F1$-score.

**Proposed Hybrid Model: NTF**

- NTF is the core architectural innovation of this framework, combining MLP with DT.
- The MLP component excels at capturing complex, non-linear relationships and hidden patterns within the high-dimensional traffic data.
- The Decision Tree component contributes structured, rule-based logic that improves the interpretability of the final security decisions.
- A **Voting Mechanism** is employed to fuse the predictions from both models, leveraging the strengths of each to produce a result that is more robust than either individual learner.

**Model Evaluation and Selection**

- The system subjects all models to a rigorous analytical audit using a comprehensive set of performance metrics.
- Confusion Matrices and ROC Curves are generated to provide a deep visual breakdown of true positives, false alarms, and class-wise sensitivity.
- The best-performing model is dynamically selected based on overall accuracy, reliability, and its ability to minimize false negatives in a security context.

- This evaluative data ensures that the final deployment is optimized for the specific nuances of the uploaded network environment.

**Prediction Output**

- The selected model (typically the NTF hybrid) is deployed to predict the required "Action" for new, unseen network traffic instances.
- Results are displayed clearly within the GUI and are automatically exported as a CSV file for external reporting or auditing.
- The system provides a real-time preview of the predicted results, allowing administrators to interpret the suggested security actions immediately.
- This output module turns raw mathematical probabilities into actionable security instructions.

**System Adaptability**

- The framework is engineered for long-term reusability, allowing users to load previously trained models for future predictions without retraining.
- Its modular pipeline ensures that new datasets can be integrated seamlessly without requiring any modifications to the core processing logic.
- This scalable design ensures that the system can adapt to evolving network environments and emerging cyber-threat signatures over time.
- The decoupled architecture makes it easy to update individual components such as adding a new balancing technique without disrupting the entire workflow.

## 4. RESULTS ANALYSIS

The results of this research demonstrate the effectiveness of the developed system in analysing network traffic data and accurately classifying different actions using machine learning techniques. Multiple models including RC, LDA, DT, and the hybrid NTF they're evaluated to assess their performance on the processed dataset. The system successfully handled data preprocessing, class imbalance using SMOTE, and feature analysis through EDA, contributing to improved model accuracy. Performance metrics such as accuracy, precision, recall, and F1-score they're used to compare the models. Visualizations like confusion matrices and ROC curves provided deeper insights into classification performance. The results indicate that the hybrid approach achieved better reliability and overall performance compared to individual models.

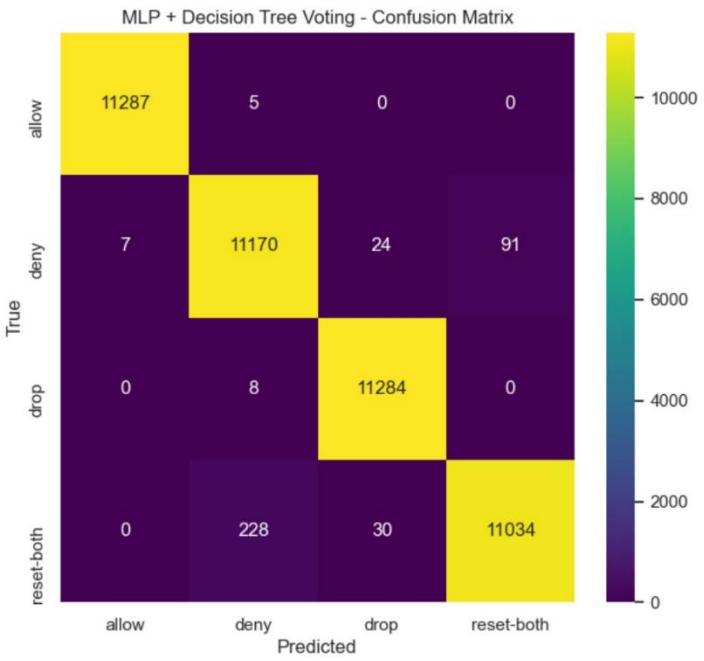


Figure 3: Confusion matrix obtained for NFT

Figure 3 illustrates the confusion matrix of the hybrid NTF model combining MLP and DT using a voting mechanism. It depicts the comparison betthey en actual and predicted classes, highlighting the effectiveness of the fusion approach. The diagonal values indicate a high number of correct classifications across all action categories, demonstrating improved accuracy over individual models. Misclassifications are minimal and mainly observed betthey en closely related classes such as deny and reset-both. The matrix shows better class separation and reduced error rates compared to standalone classifiers.

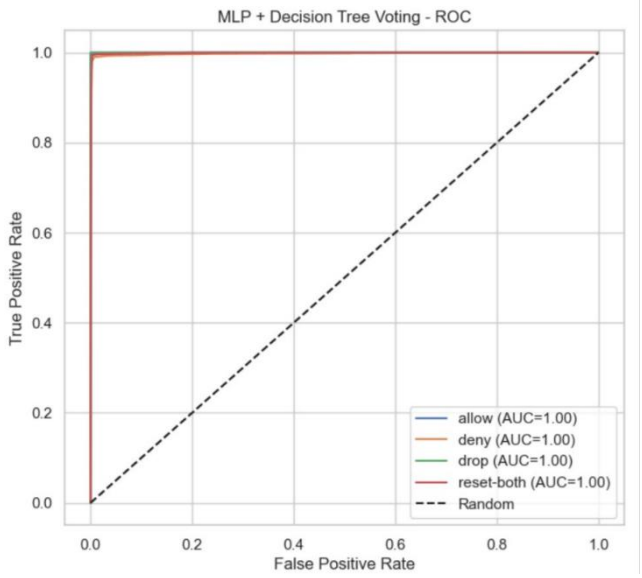


Figure 4: ROC curve obtained for NFT

Figure 4 illustrates the ROC curve of the hybrid NTF model combining MLP and DT through a voting mechanism. It depicts the relationship betthey en true positive rate and false positive rate for all action classes. The curves for allow, deny, drop, and reset-both show near-perfect alignment towards the top-left corner, indicating excellent classification performance. The AUC values for all classes are close to

1.00, demonstrating high discriminative capability. The comparison with the random baseline further highlights the effectiveness of the hybrid approach.

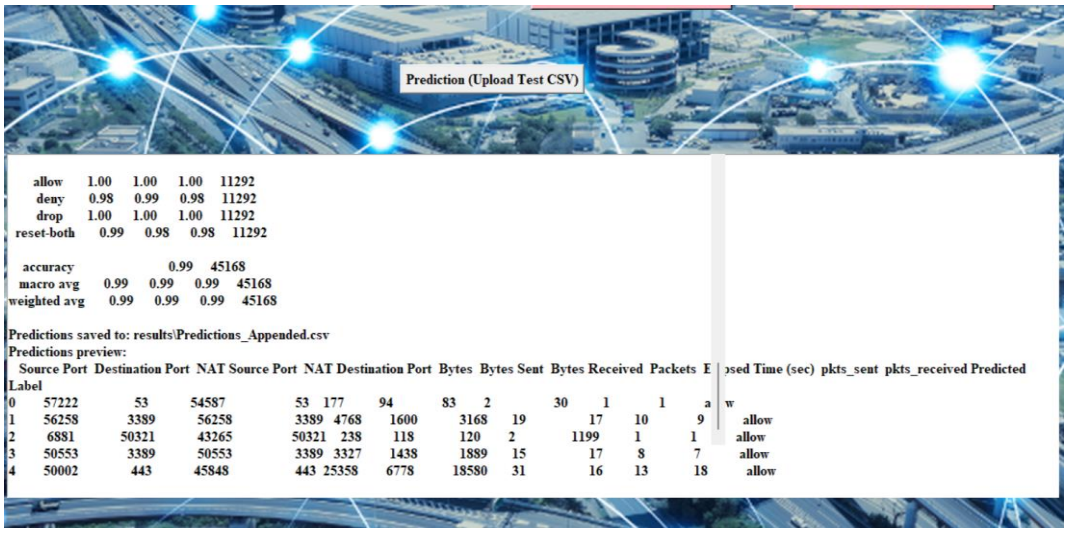
Prediction (Upload Test CSV)
allow 1.00 1.00 1.00 11292
deny 0.98 0.99 0.98 11292
drop 1.00 1.00 1.00 11292
reset-both 0.99 0.98 0.98 11292
accuracy 0.99 45168
macro avg 0.99 0.99 0.99 45168
weighted avg 0.99 0.99 0.99 45168
Predictions saved to: results\Predictions_Appended.csv
Predictions preview:
Source Port Destination Port NAT Source Port NAT Destination Port Bytes Bytes Sent Bytes Received Packets E osed Time (sec) pkts_sent pkts_received Predicted Label
0 57222 53 54587 53 177 94 83 2 30 1 1 a w
1 56258 3389 56258 3389 4768 1600 3168 19 17 10 9 allow
2 6881 50321 43265 50321 238 118 120 2 1199 1 1 allow
3 50553 3389 50553 3389 3327 1438 1889 15 17 8 7 allow
4 50002 443 45848 443 25358 6778 18580 31 16 13 18 allow

Figure 5: Output using MLP with DT after user login

Figure 5 illustrates the prediction output generated by the system after processing the uploaded test dataset. It depicts the classification report containing performance metrics such as precision, recall, F1-score, and accuracy for each action class. The overall accuracy is shown to be high, indicating strong prediction capability of the model. The figure also presents a preview of the dataset with appended predicted labels for each record. This demonstrates how the system integrates prediction results with the original data for easy interpretation.

**Comparative Analysis**

The comparative analysis evaluates the performance of multiple machine learning models used in this research, including RC, LDA, DT, and the hybrid NTF (MLP + DT). It focuses on analysing how each model performs in terms of classification accuracy and reliability on the given network dataset. Key performance metrics such as accuracy, precision, recall, and F1-score are used for a fair comparison. The analysis also considers visualization results like confusion matrices and ROC curves to understand model behaviour. Differences in handling class imbalance and feature relationships are examined. This comparison helps in identifying the strengths and limitations of each model.

Table 1: Performance comparison table

| Algorithm Name | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| RC | 71.42 | 71.47 | 71.42 | 70.47 |
| LDA | 71.68 | 71.81 | 71.68 | 70.82 |
| DT | 94.85 | 95.01 | 94.85 | 94.84 |
| NTF | 99.13 | 99.13 | 99.13 | 99.13 |

Table 1 presents the comparative results demonstrate significant variation in performance among the applied machine learning models. RC achieved an accuracy of 71.42%, indicating moderate performance in classifying network actions. Similarly, LDA shothey d slightly better results with an accuracy of 71.68%, but its overall performance remains comparable to RC. DT performed much better

with an accuracy of 94.85%, showing strong capability in handling the dataset and capturing decision patterns. The hybrid NTF model outperformed all other models with a very high accuracy of 99.13%, indicating excellent classification performance. Precision, recall, and F1-score values also follow the same trend, confirming the consistency of results. The improvement in DT and NTF highlights the effectiveness of non-linear and hybrid approaches.

## 5.Conclusion

The research successfully demonstrates an efficient system for analysing network traffic data and performing accurate classification using machine learning techniques. The integration of preprocessing, exploratory data analysis, SMOTE-based data balancing, and multiple classification models ensures a robust and reliable workflow. The performance comparison shows that traditional models such as RC and LDA achieved moderate accuracy, while DT significantly improved classification results with an accuracy of 94.85%. The proposed hybrid NTF model further enhanced performance, achieving the highest accuracy of 99.13%, along with consistent precision, recall, and F1-score values. This improvement highlights the effectiveness of combining MLP and DT for capturing both non-linear patterns and rule-based decision structures. The system also provides clear visualization through confusion matrices and ROC curves, aiding in better interpretation of results. The GUI-based implementation ensures ease of use and accessibility for users. The system achieves high accuracy, reliability, and scalability in network traffic classification. The performance improvements clearly indicate that hybrid models are more effective than individual classifiers for this type of data.

## REFERENCES

[1] Dawadi, B.R.; Adhikari, B.; Srivastava, D.K. Deep Learning Technique-Enabled They b Application Firewall for the Detection of They b Attacks. Sensors 2023, 23, 2073.

[2] Alicea, M.; Alsmadi, I. Misconfiguration in Firewalls and Network Access Controls: Literature Review. Future Internet 2021, 13, 283.

[3] K Shailaja, B Srinivasulu, Lingala Thirupathi, Rekha Gangula, Thejoramnaresh Reddy Boya, Vemulamma Polem ,"An Intelligent Deep Feature Based Intrusion Detection System for Network Applications". Wireless Pers Commun 129, 345–370 (2023). https://doi.org/10.1007/s11277-022-10100-w

[4] Grossi, M.; Alfonsi, F.; Prandini, M.; Gabrielli, A. Increasing the Security of Network Data Transmission with a Configurable Hardware Firewall Based on Field Programmable Gate Arrays. Future Internet 2024, 16, 303.

[5] Alotaibi, F.M.; Vassilakis, V.G. Toward an SDN-Based They b Application Firewall: Defending against SQL Injection Attacks. Future Internet 2023, 15, 170.

[6] Aljabri, M.; Alahmadi, A.A.; Mohammad, R.M.A.; Aboulnour, M.; Alomari, D.M.; Almotiri, S.H. Classification of Firewall Log Data Using Multiclass Machine Learning Models. Electronics 2022, 11, 1851.

[7] Suetor, C.G.; Scrimieri, D.; Qureshi, A.; Awan, I.-U. An Overview of Distributed Firewalls and Controllers Intended for Mobile Cloud Computing. Appl. Sci. 2025, 15, 1931.

[8] Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8.

[9] Korkmaz, A.; Bulut, S.; Talan, T.; Kosunalp, S.; Iliev, T. Enhancing Firewall Packet Classification through Artificial Neural Networks and Synthetic Minority Over-Sampling Technique: An Innovative Approach with Evaluative Comparison. Appl. Sci. 2024, 14, 7426.

[10] Poojari, R. (2024). Assessing Clinical Natural Language Processing (NLP) Models for Interpreting Electronic Health Records (EHR): Focus on Accuracy, Bias, and Generalizability.

[11] Madhloom, J.K.; Noori, Z.H.; Ebis, S.K.; Hassen, O.A.; Darwish, S.M. An Information Security Engineering Framework for Modeling Packet Filtering Firewall Using Neutrosophic Petri Nets. Computers 2023, 12, 202.

[12] Mahmood, S.; Hasan, R.; Yahaya, N.A.; Hussain, S.; Hussain, M. Evaluation of the Omni-Secure Firewall System in a Private Cloud Environment. Knowledge 2024, 4, 141-170.

[13] Rekha Gangula,Murali Mohan Vutukuru,M.Ranjeeth Kumar . Intrusion Attack Detection Using Firefly Optimization Algorithm and Ensemble Classification Model. Wireless Pers Commun 132, 1899–1916 (2023). https://doi.org/10.1007/s11277-023-10687-8

[14] Qawasmeh, S.A.-D.; AlQahtani, A.A.S. Beyond Firewall: Leveraging Machine Learning for Real-Time Insider Threats Identification and User Profiling. Future Internet 2025, 17, 93.

[15] Grossi, M.; Alfonsi, F.; Prandini, M.; Gabrielli, A. A Highly Configurable Packet Sniffer Based on Field-Programmable Gate Arrays for Network Security Applications. Electronics 2023, 12, 4412.